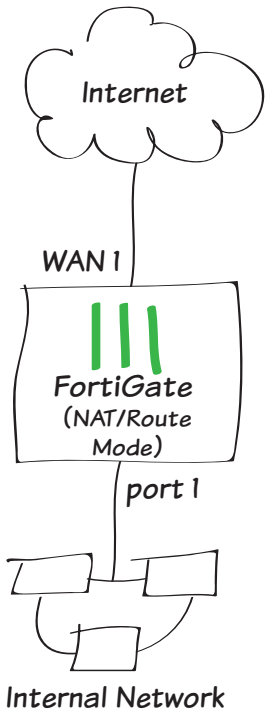
Connecting a private network to the Internet using NAT/Route mode

In this example, you will learn how to connect and configure a new FortiGate unit in NAT/Route mode to securely connect a private network to the Internet.

In NAT/Route mode, a FortiGate unit is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiGate to hide the IP addresses of the private network using network address translation (NAT).

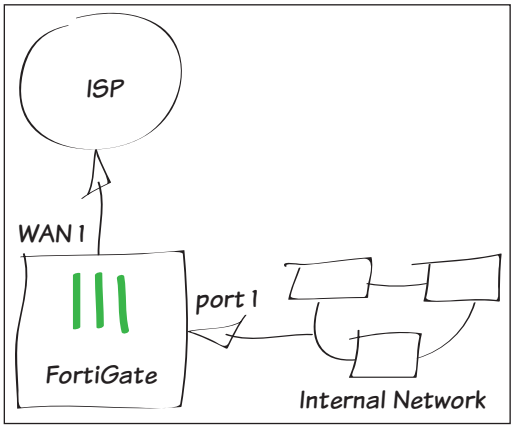
1. Connecting the network devices and logging onto the FortiGate
2. Configuring the FortiGate's interfaces
3. Adding a default route
4. (Optional) Setting the FortiGate's DNS servers
5. Creating a policy to allow traffic from the internal network to the Internet
6. Results



1. Connecting the network devices and logging onto the FortiGate

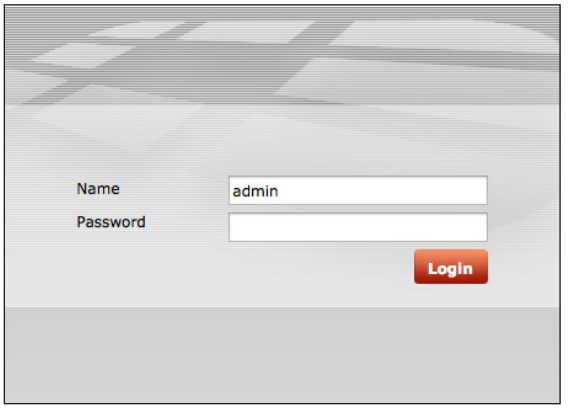
Connect the FortiGate's Internet-facing interface (typically WAN1) to your ISP-supplied equipment and Connect a PC to the FortiGate using an internal port (typically port 1).

Power on the ISP's equipment, the FortiGate unit, and the PC on the internal network.



From the PC on the internal network, connect to the FortiGate's web-based manager using either FortiExplorer or an Internet browser (for information about connecting to the web-based manager, please see your models QuickStart Guide).

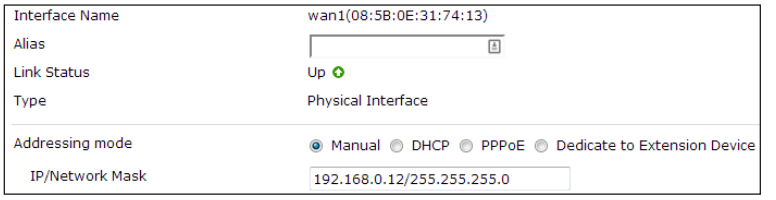
Login using an admin account (the default admin account has the username admin and no password).



2. Configuring the FortiGate's interfaces

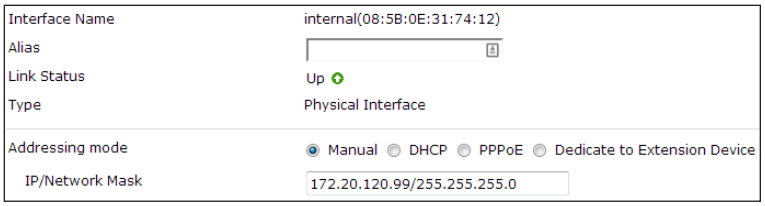
Go to **System > Network > Interfaces** and edit the Internet-facing interface.

Set **Addressing Mode** to **Manual** and the **IP/Netmask** to your public IP address.



Edit the **internal** interface (called **lan** on some FortiGate models).

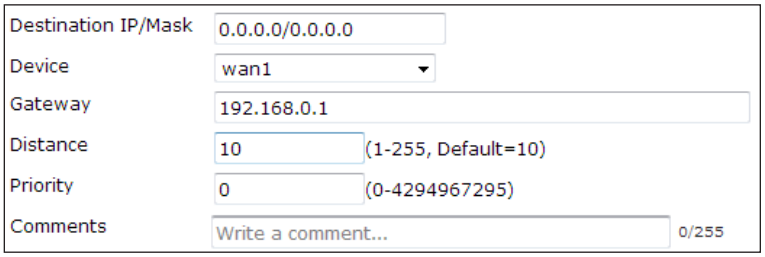
Set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the private IP address you wish to use for the FortiGate.



3. Adding a default route

Go to **Router > Static > Static Routes** (or **System > Network > Routing**, depending on your FortiGate model) and create a new route.

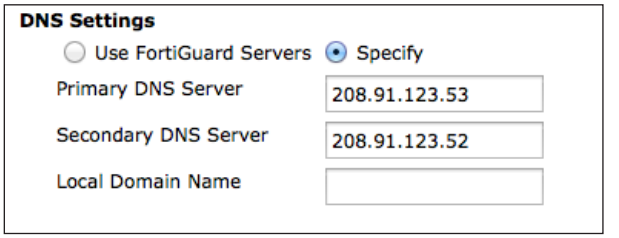
Set the **Destination IP/Mask** to 0.0.0.0/0.0.0.0, the **Device** to the Internet-facing interface, and the **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements.



A default route always has a Destination IP/Mask of 0.0.0.0/0.0.0.0. Normally, you would have only one default route. If the static route list already contains a default route, you can edit it or delete it and add a new one.

4. (Optional) Setting the FortiGate's DNS servers

The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.



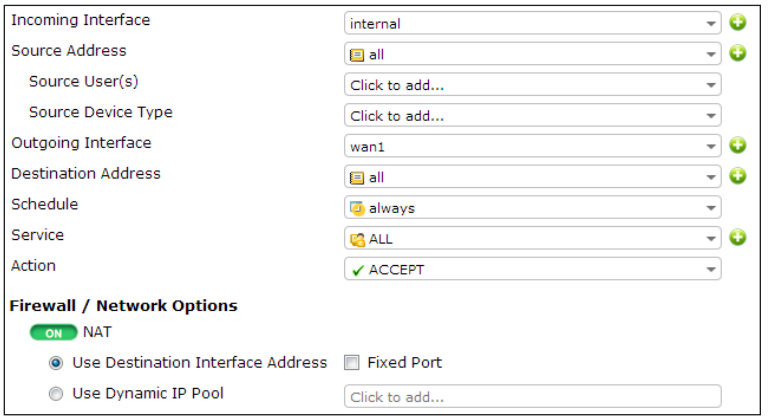
5. Creating a policy to allow traffic from the internal network to the Internet

Some FortiGate models include an IPv4 security policy in the default configuration. If you have one of these models, edit it to include the logging options shown below, then proceed to the results section.

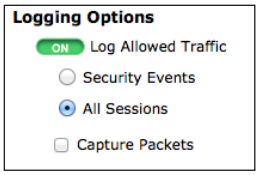
Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

Set the **Incoming Interface** to the **internal** interface and the **Outgoing Interface** to the Internet-facing interface.

Make sure the **Action** is set to **ACCEPT**. Turn on **NAT** and make sure **Use Destination Interface Address** is selected.



Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



6. Results

You can now browse the Internet using any computer that connects to the FortiGate's internal interface.

You can view information about the traffic being processed by your FortiGate by going to **System > FortiView > All Sessions** and finding traffic that has the **internal** interface as the **Src Interface** and the Internet-facing interface as the **Dst Interface**.

If these two columns are not shown, right-click on the title row, select **Src Interface** and **Dst Interface** from the dropdown menu, and then select **Apply**.

#	Date/Time	Dst Interfa...	Src Interfa...	Destination	Sent / Received
1	13:10:25	wan1	lan	8.247.14.128 (static.licdn.com)	1.10 KB / 640 B
2	13:10:25	wan1	lan	138.108.6.20 (secure-us.imrworldwide.com)	1.05 KB / 4.29 KB
3	13:10:24	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	967 B / 444 B
4	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	2.28 KB / 3.81 KB
5	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	3.34 KB / 5.83 KB
6	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	3.52 KB / 16.20 KB
7	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	3.89 KB / 26.95 KB
8	13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	6.03 KB / 32.48 KB
9	13:10:20	wan1	lan	208.91.114.158 (blog.fortinet.com)	1.26 KB / 2.22 KB
10	13:10:19	wan1	lan	8.247.14.128 (static.licdn.com)	1.46 KB / 885 B
11	13:10:19	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	1.58 KB / 710 B
12	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	5.71 KB / 3.19 KB
13	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	5.54 KB / 3.19 KB
14	13:10:17	wan1	lan	194.122.82.32 (www.google.ca)	184 B / 92 B
15	13:10:17	wan1	lan	194.122.82.32 (www.google.ca)	184 B / 92 B
16	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	4.98 KB / 2.80 KB
17	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	8.01 KB / 4.69 KB
18	13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	5.96 KB / 3.17 KB
19	13:10:16	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	1.02 KB / 496 B
20	13:10:16	wan1	lan	173.194.43.84 (www.google.com)	272 B / 164 B